Policy 1.1.7

E-MAIL USAGE

Contact: Contracts and Legal Affairs Manager

1.1.7.1 Purpose

DIS provides electronic mail (e-mail) technology for official business use that supports the agency's goals and priorities. The purpose of this policy is to set forth the proper business and personal use of e-mail by employees. This policy applies not only to DIS employees but also to contractors, interns, and other individuals who have been given authorized access to the DIS e-mail system.

1.1.7.2 Definitions

"Confidential information" means information exempt from disclosure under Chapter 42.17 RCW, the Public Records Act, or other state or federal law, including but not limited to trade secrets, valuable formulae, research data, and computer source code.

"DIS Privacy Officer" means the individual appointed by DIS pursuant to Governor's Executive Order 00-03 to handle complaints, questions and recommendations from, and provide information to, the public on the collection and use of personal information.

"DIS Public Disclosure Officer" means the individual appointed by DIS pursuant to Washington Administrative Code section 143-06-060 to be primarily responsible for responses to requests for public records.

"DIS Records Officer" means the individual appointed by DIS pursuant to RCW 40.14.040 to oversee and coordinate the DIS records management program.

"E-mail System" means an electronic mail system that provides the means for creating messages, transmitting them through a network, and displaying the messages on the recipient's workstation, personal computer (PC), terminal, or other device.

"Encryption" means a method of "scrambling" data using a cryptographic algorithm based on a secret key.

"Forgery" means sending messages from the e-mail address of another person or attempting to disguise a person's identity when sending e-mail. This includes modifying received or to-be-forwarded e-mail to remove or change the author's name, or modifying the content of information to be forwarded so as to alter the intent of the message.

APPROVED
Executive Ethics Board
Date: 4/11/03

"Personal information" means information collected by DIS about an individual that is readily identifiable to that specific individual, including but not limited to social security number, home address, home telephone number, and financial information.

"Proprietary information" means information provided by a vendor that the vendor has indicated is confidential. Such information includes trade secrets and valuable formulae.

1.1.7.3 Risk Statement

The improper or illegal use of e-mail may result in serious risk and liability to both DIS and the individual employee. These risks include but are not limited to:

- Loss of public trust in DIS and state government
- Interference with performance and services
- Loss of network or operational integrity
- Financial loss
- Personal and agency liability

Employees must be aware that e-mails are public records that are reproducible, are not private, and may be subject to disclosure under the public disclosure laws. Only send e-mails with content that can be displayed on a public notice board.

1.1.7.4 Business and Limited Personal Uses

The DIS e-mail system is provided to employees as a productivity tool for conducting state business. Employees are required to use the e-mail system in performing their official duties. Employees' use of e-mail must be conducted in a manner that is consistent with public service and trust.

Employees may make occasional but limited use of the DIS e-mail system for purposes other than the conduct of official duties provided that the use conforms to the limited personal use standards. The permitted uses for a purpose other than the conduct of official duties requires that the use meet all of the following requirements as interpreted by the Executive Ethics Board:

- Results in little or no cost to the state
- Is infrequent
- Is brief in duration
- Is the most effective use of time and resources
- Does not interfere with the performance of official duties
- Does not disrupt other state employees
- Does not obligate other state employees to make a personal use of state resources, and
- Does not compromise the security or integrity of state property, information, or software

APPROVED
Executive Ethics Board
Date: 4/11/03

1.1.7.5 Prohibited Uses

In the course of using the DIS e-mail system for either business or limited personal uses, employees are prohibited from:

- Sending or forwarding e-mails that contain inappropriate content that includes libelous, defamatory, offensive, racist, obscene, or pornographic content
- Discriminating against or harassing another person
- Supporting, promoting or soliciting for an outside organization unless authorized by the director and permissible by law
- Forging or attempting to forge e-mail messages
- Conducting or supporting an outside job or business
- Utilizing for commercial use, such as advertising, selling, and promoting, that is not related to official duties
- Campaigning or political use
- Forwarding chain e-mails, junk mail, and jokes
- Sending or forwarding mass mailings
- Conducting activities prohibited by state laws and rules
- Engaging in actions that violate any DIS policy

When using the DIS e-mail system for a purpose other than the conduct of official duties, employees, under any circumstances, are prohibited from using the e-mail system where that use involves state property that has been removed from an official duty station. Employees are not to allow others, such as family members and friends, to use state resources under their control. State regulations prohibit employees from using state resources for personal purposes and then reimbursing the state for the cost incurred. If a violation of these regulations occurs, the employee will be required to reimburse DIS, but the reimbursement does not cure the violation.

1.1.7.6 No Expectation Of Privacy

DIS has the right to access, inspect, or monitor any state resource, and that includes an employee's use of the DIS e-mail system. Employees cannot expect privacy in their use of the e-mail system, whether that use occurs in the conduct of official duties or is a use made for a purpose other than the conduct of official duties. Since the DIS e-mail system is a state resource, DIS is not required to provide notification to or seek permission from employees prior to accessing, inspecting or monitoring employees' use of the system.

While DIS does not regularly monitor e-mail messages, employees are on notice that:

- The maintenance and operation of electronic message systems may result in observation of random messages
- Managers with appointing authority approval may monitor messages
- Managers may access and retrieve data under employees' control

1.1.7.7 Reporting Misuse

APPROVED
Executive Ethics Board
Date: 4/11/03

Employees who discover misuse of the DIS e-mail system shall immediately report such misuse to their supervisors. It is not a violation of this policy for DIS employees to forward e-mail messages to their managers, supervisors, and other individuals to report misuse.

1.1.7.8 Controlling Access to E-mail

Employees are responsible for protecting e-mail messages and systems from unauthorized access by securing communications devices to the extent possible. Employees should not provide others access to their e-mail account by sharing passwords or leave their workstation unattended for long periods without securing the workstation. Additionally, employees should use readily available security tools, such as a password-protected screen saver, to control access to their workstations and laptops.

1.1.7.9 Public Records Retention

E-mail messages are simply another type of public record. E-mail messages that are sent or received, that contain information about business activities, and that can function as evidence of business transactions are part of the records of DIS and are subject to the guidelines in the Public Records Act, Chapter 40.14 RCW, which regulates the preservation and destruction of public records. For the purposes of satisfying public record laws, e-mail is defined as not only the messages sent and received by e-mail systems, but also transmission and receipt transaction data as well. The content, transactional information, and any attachments associated with the message are considered a record.

E-mail messages that are public records should be kept for the retention period identified on either the state's general records retention schedule or a DIS specific retention schedule. In addition, there may be reasons to retain these records longer for ongoing operations, audits, legal proceedings, research, or other known purpose. For more information on records retention matters, please refer to the Secretary of State General Records Retention Schedules or contact the DIS Records Officer.

To assure appropriate retention of public records generated or received through an e-mail system, it is recommended that you transfer messages and attachments to paper, disk, or LAN (network) drive. E-mail should be considered a communication tool, not a storage mechanism. Retention is the responsibility of the sender and receiver of the message, not the back-up process. Back-up copies performed by the LAN staff are NOT records retention. If employees are in doubt about the retention of an e-mail message, they need to contact the DIS Records Officer or divisional coordinators to determine who has the primary records retention responsibility.

1.1.7.10 E-Mail Encryption

APPROVED
Executive Ethics Board
Date: 4/11/03

Regardless of whether or not the technology is available for doing so, employees should exercise extreme discretion in determining whether e-mail should be encrypted. Should the confidential nature of an e-mail message warrant encryption, encryption should be performed using only those encryption tools and/or systems that provide for back up of the recipient's private (decryption) key. Whenever possible, e-mail should be encrypted using secure e-mail systems intended for this specific purpose.

1.1.7.11 Confidential, Personal And Proprietary Information

DIS supports open government and the public disclosure laws of this state. However, in accordance with other state and federal laws, DIS is also committed to protecting confidential, personal and proprietary information that may be contained in public records. Therefore, DIS employees shall ensure that all public records that contain confidential, personal or proprietary information are clearly marked "Confidential" or "Proprietary".

Avoid sending confidential, personal or proprietary information by e-mail. If you do, you should secure the information by including it in a Microsoft Word or Excel file and protecting it with a password. Then provide the recipient with the password by means of other communication, for instance by telephone. For additional information on maintaining public records that contain confidential, personal or proprietary information, employees should consult the DIS Public Disclosure Officer and DIS Privacy Officer.

1.1.7.12 Public Records Disclosure

The intent of the Public Records Act is to provide public access to records and protect public records from damage or destruction. DIS is required to make available for public inspection and copying all public records, unless the record falls within the specific exemptions of the Revised Code of Washington or other statute that exempts or prohibits disclosure of specific information or records. If you receive a public records request, please immediately forward that request to the DIS Public Disclosure Officer.

In addition, no employee may use or copy confidential, personal or proprietary information for his or her own personal purposes or disclose public records containing confidential, personal or proprietary information to any person other than a person legally authorized to obtain the information. Employees may, in the course of their official duties, copy, use or disclose public records containing confidential, personal or proprietary information in order to accomplish a specific authorized purpose. Third party requests for public records that contain confidential, personal or proprietary information should immediately be forwarded to the DIS Public Disclosure Officer.

1.1.7.13 Violation Warning

Violations of this policy may result in agency disciplinary action up to and including dismissal and legal action. In addition, there may also be separate actions against the employee for violation of the state's ethics law, criminal prosecution, and civil actions.

APPROVED
Executive Ethics Board
Date: 4/11/03

References

DIS Policy 1.1.4 – Use of State Resources

DIS Policy 1.1.5 – Confidentiality of Customer Information

DIS Policy 4.2.3 – Public Disclosure - Vendor Bids and Scores

DIS Policy 5.1.2 – Public Disclosure

DIS Policy 5.1.3 – Records Disposition Management

DIS Policy 6.2.2 – Intellectual Property Protection

DIS Policy 7.2.1 – Handling and Disposal of Public Records Containing Confidential Information

Chapter 40.14 RCW - Preservation and Destruction of Public Records

RCW 42.17.250 et seq. - Public Records Act

WAC 292-110-010

General Records Retention Schedules

Executive Ethics Board